



Freedom of Information Act Publication Scheme	
Protective Marking	Not Protectively Marked
Publication Scheme Y/N	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>
Title	Information Management in the MPS.
Version	Version 4.1
Summary	This policy provides a framework for the management and control of MPS information assets, whatever the format.
Branch / OCU	Enterprise Architecture Board (EAB)
Author	Directorate of Information (DoI)
Date created	February 2011
Review date	February 2014

Introduction

This policy relates to the management and control of MPS information assets. The term information asset includes both the information itself, plus the systems and processes that deal with the information. In this context the word data is synonymous with information. MPS information exists in different formats to support business need, including paper documents ['hard copies']; electronically held computer information [i.e. digital/ 'soft copy']; or other means such as photographic media. MPS information is classified, utilised and protected according to value and policing requirements, such as criminal records or intelligence purposes.

Application

This policy comes into immediate effect.

All police officers and police staff, including the extended police family, those working voluntarily or under contract to the Metropolitan Police Authority (MPA) and where appropriate our partners, must be aware of, and are required to comply with, all relevant MPS policy and associated procedures.

This policy applies in particular to officers and staff who have defined responsibilities for ensuring that their personnel are appropriately briefed on Information Management (IM) policy.

This is most pertinent to the following roles:

- Borough Operational Command Unit (BOCU) commanders
- OCU commanders
- Heads of branches
- All line managers
- Information Managers and decision makers

N.B. This list is not intended to be exhaustive.

Purpose

The policy is designed to support the delivery of information management (IM) across all policing functions to achieve a safer London. To further the primary aim, the policy is designed for application and compliance with technical, professional standards and the relevant legal requirements. To achieve the purpose the policy and supporting standard operating procedures (SOPs) provides instructions and guidance to personnel for the proper management and control of MPS information assets.

Scope

This policy, that supports the IM Strategy, relates to the management and security of information and systems across all policing and support activity.

It applies to all MPS employees and representatives in both a professional and private capacity. This policy implies a general requirement of due diligence/ care to be applied by all individuals and also whether or not managerial or non-managerial roles are involved. It is relevant in respect of all MPS information, held in whatever format, and the systems and processes designed to record and store such information.

Policy Statement

- The MPS will manage information to ensure that, subject to appropriate security considerations, it is readily available to all those who need to use it in their work
- The MPS will manage information to ensure that, subject to appropriate security considerations, it is made available to the public in an accessible and easily understandable manner
- SOPs will exist to provide effective, efficient and legally compliant procedures for the creation, use, maintenance, integrity, safekeeping, retention and disposal of all MPS information assets
- The MPS will promote the measures highlighted in these SOPs to ensure that all users of MPS information are made aware of their responsibilities in the management of such information
- All MPS staff and others who create, use, manage, protect, exploit or dispose of information must do so in accordance with these SOPs.

Benefits

IM policy will enable the MPS to:

- Apply effective, efficient and legally compliant procedures for the creation, use, safekeeping, maintenance, integrity, retention and disposal of all MPS records;
- Provide an audit trail of activities and thereby provide an indispensable element of accountability and compliance;
- Manage MPS information in such a way as to ensure that, subject to appropriate security considerations, information is readily available to those that need to use it in their work; and
- Achieve the earliest possible disposal of our recorded information commensurate with the business need and statutory retention requirements.

MPS Information Management Policy consists of a number of inter-related and linked components, as follows:

Information Management

This policy and associated SOPs cover the following elements that relate to all MPS information:

- MPS security procedures;
- Enterprise Architecture [*i.e. the Enterprise Architecture Practice, Directorate of Information, sets the standards to be applied in developing ICT infrastructure and systems in the MPS*];
- Records management;
- Data quality;
- Legal compliance; and
- Information sharing with partner organisations.

N.B. This list is not intended to be exhaustive.

Management of Police Information (MoPI)

This policy governs MPS compliance with the statutory Code of Practice [issued under the Police Acts 1996 & 1997] and the supporting **Guidance on the Management of Police Information (MoPI) 2nd edition 2010**.

MoPI focuses on a subset of MPS information. This subset of information is known as "police information" and is defined by MoPI as the information required for a policing purpose.

Information Security

There is a fundamental requirement that all MPS information is afforded appropriate protection, commensurate with its value and the risks associated with its potential loss or compromise. Information security is based on the practical application of risk assessment methodologies, applied to protect information and assure the systems which hold the information.

As with other UK police services, the MPS is mandated to manage its information securely by application of the Association of Chief Police Officers (ACPO) [for the police service in England, Wales & Northern Ireland] & Association of Chief Police Officers Scotland (ACPOS) **Information Systems Community Security Policy (CSP)**. CSP includes Her Majesty's Government (HMG) information assurance standards to be followed for Information Communications and Technology (ICT) systems and information processing in the public sector [including police forces]. Specifically, CSP requires forces to demonstrate standards of assurance that allows secure connection to national police systems.

Information security incidents and other information risk issues are to be reported using the **Security Incident Reporting, Handling & Investigation**

Standard Operating Procedures (SOPs) and escalated as appropriate for professional advice and remedial action.

The information security element of this policy, combined with the policies below, set out complete instructions for MPS security.

The four policies are:

- Vetting [Personnel Security];
- Business Risk management;
- Business Continuity; and
- Security of the MPS estate.

Information Management Governance

The Directorate of Information (DoI) is responsible for the delivery of MPS ICT systems and services. The Director of Information is designated the MPS Chief Information Officer (CIO) and the Senior Information Risk Owner (SIRO) for the organisation and reports on these matters as a member of Management Board.

The **Information Governance Framework (IGF)** defines the hierarchy, structure and key roles necessary for the governance of information holdings and information systems in the MPS. The IGF sets out the main roles and responsibilities of MPS personnel in the delivery of information management whether that involves information held or recorded on electronic computer databases or in alternative formats [e.g. paper based files].

Policy & SOPs approval

Oversight and development of the MPS information security element of this policy is the responsibility of the Departmental Security Officer (DSO) reporting to the METSEC [MPS Security] Board. The Enterprise Architecture Board (EAB) is the forum that approves IM policy and all SOPs. Both of these boards are DoI strategic forums with additional representation drawn from across key MPS business groups.

The IM Policy Statement has been reviewed and there are no identified Health & Safety issues which impact on this policy.

Responsibilities

Ownership	Director of Information
Approval	Enterprise Architecture Board (EAB)
Implementation	Security, Standards & Architecture, DoI2
Monitoring & Compliance	Information Compliance, DoI2(3)
Reviewer	Information Assurance Unit, DoI2(3-1)

Associated Documents and Policies

Procedures supporting the IM policy are contained in Information Management SOPs.

These include:

Enablers:

- The METSEC Code [the MPS Security Code Manual]
- Information Code of Conduct & supporting Frequently Asked Questions (FAQs) [*located on the AWARE/ Foundation desktop*]
- Information Governance Framework (IGF)
- Information Policy Framework (IPF)

Security:

- Audit Trail SOPs
- AWARE Accounts for non-MPS Personnel SOPs
- ICT Equipment Funded by Non-MPS Sources, Donated or Procured Locally - Information Security Requirements SOPs [*under review*]
- Installation of Network Connections Outside the MPS SOPs [*under review*]
- Management of Connections to / within the MPS Technology Infrastructure (MTI) SOPs [*under review*]
- Mobile Computing Security SOPs
- Personal Use of MPS Information, Communications and Technology Systems SOPs [*under review*]
- Repair, Re-Use and Disposal of Hardware and Media SOPs
- Secure External Gateway - New External Connections SOPs [*under review*]
- Security Incident Reporting, Handling and Investigation SOPs
- Third Party Code of Connection SOPs [*under review*]
- Use of the Internet in the MPS SOPs
- Working Away from the Office SOPs

For advice on interpretation of security SOPs and all compliance issues, visit Information Assurance

Legislative:

- Data Protection Act 1998 (DPA) Compliance SOPs
- Data Protection Act 1998 (DPA) Compliance Standard for International Data Processing SOPs
- Compliance with the Freedom of Information Act, 2000 SOPs
- Information Sharing with Partner Organisations SOPs

Information & Records Management:

- Intranet Publishing SOPs
- METRIC - Managing Correspondence Received by the MPS SOPs
- Records Management
- Registration of Crime Files SOPs

Process:

- Technology & Radio Equipment Rooms (TER) Policy & Requirements SOPs
- Videoconferencing Risk Assessment SOPs [*under review*]

Related SOPs:

- Physical Security Building Standards SOPs
- Vetting SOPs

Forms:

- Application for an Access Control Package Form
- Confidential Agreement Form
- Protective Marking System - PMS Leaflet
- Security Incident Report Form

Links to other MoPI-related policies / SOPs / documents:

- Crime Management Units Minimum Model Policy
- Custody Policy
- Domestic Violence Policy
- Firearms Licensing Policy
- Management of MPS Intelligence Policy
- MPS Intelligence Manual
- Child Abuse Investigation Policy
- Investigative Interviewing Policy
- Safeguarding Adults at Risk Policy

N.B. This list cannot be exhaustive as it is possible that any document dealing with 'police information' could be referenced. The Corporate Policy Database should be searched as necessary.

Withdrawn Notices, SOPs & other documentation

The following Notices, SOPs and documents are now cancelled:

- Item 3, Notices 37/07, 12 September 2007 - Information Management in the MPS Policy Statement v3

And

- Locally Developed Systems SOPs
- Malicious Software Protection SOPs
- Public Communications Security SOPs
- Role of the Security Assurance Co-ordinator (SyAC) SOPs
- Software Compliance SOPs
- TERs, Accommodation Specifications SOPs
- TERs, Management and Control Processes SOPs

Workstation Switches Assurance Requirements SOPs